

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-102734

(43)Date of publication of application : 16.04.1996

(51)Int.Cl.

H04L 9/00

H04L 9/10

H04L 9/12

G09C 1/00

(21)Application number : 06-236500

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 30.09.1994

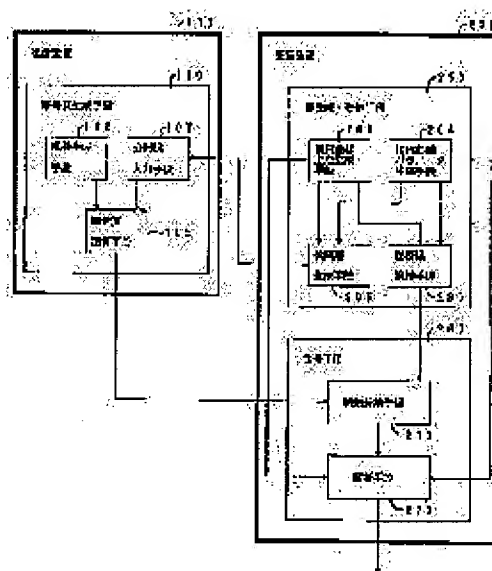
(72)Inventor : OKAMOTO TATSUAKI

(54) PUBLIC KEY CRYPTOGRAPHIC METHOD/SYSTEM

(57)Abstract:

PURPOSE: To attain the ciphering by means of a single cryptogram by using the double cycle, i.e., the characteristic of an elliptical curve to use one of both cycles for the ciphering of a written message and the other cycle for the generation of random numbers in terms of probability respectively.

CONSTITUTION: In a public key cryptographic system that assures the communication secret between a transmission device 100 and a reception device 200, a public key is generated by means of an operation carried out on an elliptical curve. When a secret key is generated, a remainder operation and a weil pairing operation are carried out to the cryptogram received from the device 100 by means of a key generation/register means 250. Then a discrete logarithm problem is solved to the result of the weil pairing operation. Thus the cryptogram is restored into a normal message by a decoder means 260 of the device 200. In this respect the device 100 includes a cryptogram generation means 110. Then the means 250 includes a parameter generation means 204 which decides the parameters of a total number (n) and the elliptical curve, and a point generation means 203 which decides two points (G1, G2) on the elliptical curves $E_n(a, b)$ in a remainder operation that defines a synthetic number (n) as the modulus.



LEGAL STATUS

[Date of request for examination] 14.10.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or

application converted registration]

[Date of final disposal for application]

[Patent number] 3278790

[Date of registration] 22.02.2002

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-102734

(43) 公開日 平成8年(1996)4月16日

(51) Int.Cl.⁶

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 L 9/00

9/10

9/12

G 0 9 C 1/00

7259-5 J

H 0 4 L 9/ 00

Z

審査請求 未請求 請求項の数 9 O L (全 15 頁)

(21) 出願番号 特願平6-236500

(22) 出願日 平成6年(1994)9月30日

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 岡本 龍明

東京都千代田区内幸町1丁目1番6号 日

本電信電話株式会社内

(74) 代理人 弁理士 伊東 忠彦

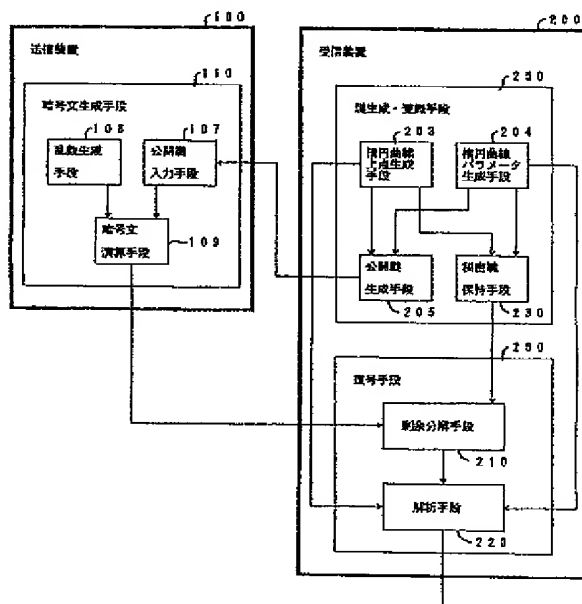
(54) 【発明の名称】 公開鍵暗号方法及び公開鍵暗号システム

(57) 【要約】

【目的】 本発明の目的は、通信効率と復号処理効率が共に工場する公開鍵暗号方法及び公開鍵暗号システムを提供することである。

【構成】 本発明は、楕円曲線上の演算を利用して生成した公開鍵を公開し、秘密鍵を生成し、保持する鍵生成・登録手段250と、送信装置100より受信した暗号文に対して剰余演算及びヴェイユ対演算を行い、ヴェイユ対演算の結果に対して離散対数問題を解くことにより暗号文を平文に復号する復号手段260とを有する受信装置200と、受信装置200から公開鍵を入手し、楕円曲線上の演算を利用して暗号文を生成する暗号文生成手段110を有する送信装置100とを具備する。

本発明の概略構成図



【特許請求の範囲】

【請求項 1】 送信装置と受信装置間の通信の秘密を保証する公開鍵暗号方法において、該受信装置側では、

楕円曲線上の演算を利用して公開鍵及び秘密鍵を生成し、

生成された該公開鍵を公開し、

生成された該秘密鍵を保持し、

該送信装置側では、

該公開鍵を入手し、

該楕円曲線上の演算を利用して暗号文を生成して、該受信装置に送信し、

該受信側装置において、

該送信装置より受信した該暗号文に対して剰余演算及びヴェイユ対演算を行い、該ヴェイユ対演算の結果に対して離散対数問題を解くことにより該暗号文を平文に復号することを特徴とする公開鍵暗号方法。

【請求項 2】 前記受信装置において、前記公開鍵及び前記秘密鍵を生成する際に、

予め合成数 n 及び前記楕円曲線のパラメータ (a, b) を定め、

さらに、該合成数 n を法とする剰余演算における楕円曲線 $E_n(a, b)$ 上の 2 点 (G_1, G_2) を定め、 k, n, a, b, G_1, G_2 を前記公開鍵とし、

該合成数 n の素因数を前記秘密鍵とする請求項 1 記載の公開鍵暗号方法。

【請求項 3】 前記送信装置において、前記暗号文を生成する際に、

乱数 γ を生成し、

該乱数 γ と入力される通信文 m を用いて、前記楕円曲線 $E_n(a, b)$ 上の前記合成数 n を法とする剰余演算における前記楕円曲線上の演算を行い、前記暗号文 c (但し、 $c = mG_1 + \gamma G_2$) を生成する請求項 1 記載の公開鍵暗号方法。

【請求項 4】 前記受信装置において、前記暗号文を復号する際に、

前記送信装置より受信した前記暗号文を前記合成数 n の素因数を法とする剰余演算の要素に分解し、

分解された要素に対して、ヴェイユ対演算を行い、該ヴェイユ対演算の演算値に対して離散対数問題を解き、該離散対数問題の解を中国人剰余定理により復号文を生成する請求項 1 記載の公開鍵暗号方法。

【請求項 5】 送信装置と受信装置間の通信の秘密を保証する公開鍵暗号システムにおいて、

楕円曲線上の演算を利用して公開鍵を生成して、公開

し、秘密鍵を生成し、保持する鍵生成・登録手段と、

該送信装置より受信した該暗号文に対して剰余演算及びヴェイユ対演算を行い、該ヴェイユ対演算の結果に対して離散対数問題を解くことにより該暗号文を平文に復号する復号手段とを有する受信装置と、

該受信装置から該公開鍵を入手し、該楕円曲線上の演算を利用して暗号文を生成する暗号文生成手段を有する送信装置とを具備することを特徴とする公開鍵暗号システム。

【請求項 6】 前記鍵生成・登録手段は、

合成数 n 及び楕円曲線のパラメータ (a, b) を定める楕円曲線パラメータ生成手段と、

該合成数 n を法とする剰余演算における該楕円曲線 E_n

(a, b) 上の 2 点 (G_1, G_2) を定める楕円曲線上点生成手段と、

該楕円曲線パラメータ生成手段により生成された該パラメータ (a, b) 及び該楕円曲線上点生成手段により生成された該 2 点 (G_1, G_2) を用いて公開鍵 $k, n,$

a, b, G_1, G_2 を生成する公開鍵生成手段と、

該合成数 n の素因数を秘密鍵として格納する秘密鍵保持手段とを含む請求項 5 記載の公開鍵暗号システム。

【請求項 7】 前記復号手段は、

該送信装置から送信された前記暗号文 c を該合成数 n の素因数を法とする剰余演算の要素に分解する剰余分解手段と、

該剰余分解手段により分解された各要素にヴェイユ対演算を用いて離散対数問題を解き、前記暗号文を復号する解析手段とを含む請求項 5 記載の公開鍵暗号システム。

【請求項 8】 前記解析手段は、

前記離散対数問題の解を中国人剰余定理により 1 つの復号文に変換する手段を含む請求項 7 記載の公開鍵暗号システム。

【請求項 9】 前記暗号文生成手段は、

前記受信装置より前記公開鍵 (k, n, a, b, G_1, G_2) を入力する公開鍵入力手段と、

乱数 γ を生成する乱数生成手段と、

該乱数生成手段により生成された該乱数 γ と入力される通信文 m を用いて前記楕円曲線 $E_n(a, b)$ 上の演算を前記合成数 n を法とする剰余演算を行い、該通信文 m を暗号文 c (但し、 $c = mG_1 + \gamma G_2$) に暗号化する暗号文演算手段を含む請求項 5 記載の公開鍵暗号システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、公開鍵暗号方法及び公開暗号鍵システムに係り、特に、電気通信システムにおいて通信の秘密を保証して通信を行う公開鍵暗号方式 (池野、小山著「現代暗号理論」電子情報通信学会) を実現する公開暗号方法及び公開鍵暗号システムに関する。

【0002】 詳しくは、デジタル化された文書を伝送する際に、楕円曲線に基づいて公開鍵暗号を用いて安全性を高めることが可能な公開暗号方法及び公開鍵暗号システムに関する。

【0003】

【従来の技術】従来の第1の公開鍵暗号を安全に実現する方法として、GoldwasserとMicaliにより確率暗号が導入されている(Goldwasser, Micali, "Probabilistic Encryption," SIAM J. Computing (1984))。

【0004】この"Goldwasser とMicali" による方法は、1ビットの情報 m (m は0か1)を

【0005】

【数1】

$$C = \begin{cases} \gamma^2 \bmod N & \text{IF } m=0 \\ a \gamma^2 \bmod N & \text{IF } m=1 \end{cases}$$

(但し、 N , a は公開鍵、 γ は乱数)

【0006】のように暗号化している。この時の暗号文は、公開鍵のサイズと同様(略500ビット)となる。

【0007】また、従来の第2の公開鍵暗号の方法として、Cohen (Cohen, Hischer, "A Robust and Verifiable Cryptographically Secure Election Scheme", Proceeding of Foundation of Computer Science, pp. 372-382 (1985) の高次剰余の理論に基づいて、より通信効率の良い方法を提案している。この方法は、 t ビットの情報 m を

$$c = a^m \cdot \gamma^L \bmod N$$

というように暗号化する(但し、 a , N , L (L のサイズは t ビット以上)は公開鍵、 γ は乱数)。この暗号文 c を復号するためには、情報 m をしらみ潰し的に探索して復号する。

【0008】

【発明が解決しようとする課題】しかし、上記の従来の第1の方法は、1ビットを暗号化すると500ビットの暗号文となり、通信効率が非常に悪いという問題がある。

【0009】また、上記の従来の第2の方法は、高次剰余の理論に基づいて上記の従来の第1の方法の問題を解決しているが、現在既知となっている全ての方法を用いても情報 m をしらみ潰し的に探索する以外に復号する方法がない。

【0010】例えば、情報 m が10ビットである場合は、 $0 \sim 2^{10} - 1$ の1024通りの全ての値を復号式に代入して満足するものを見つける必要がある。従って、現在のコンピュータの能力では、通常 2^{40} 以上になると、1日以上、 2^{60} 程度では、スーパーコンピュータを用いても何十年もかかる計算となる。従って、通常の利用環境で、数秒以内程度で復号するためには、せいぜい10ビット程度が限度である。

【0011】本発明は、上記の点に鑑みなされたもので、上記従来の問題点を解決し、通信効率と復号処理効率が共に向上する公開鍵暗号方法及び公開鍵暗号システムを提供することを目的とする。

【0012】

【課題を解決するための手段】図1は、本発明の原理を説明するためのフローチャートである。

【0013】本発明の公開鍵暗号方法は、送信装置と受信装置間の通信の秘密を保証する公開鍵暗号方法において、受信装置側では、楕円曲線上の演算を利用して公開鍵及び秘密鍵を生成し(ステップ1)、生成された公開鍵を公開し(ステップ2)、生成された秘密鍵を保持し(ステップ3)、送信装置側では、公開鍵を入手し、楕円曲線上の演算を利用して暗号文を生成し(ステップ4)、受信装置に送信し(ステップ5)、受信側装置では、送信装置より受信した暗号文に対して剰余演算及びヴェイユ対演算を行い、ヴェイユ対演算の結果に対して離散対数問題を解くことにより暗号文を平文に復号する(ステップ6)。

【0014】また、受信装置において、公開鍵及び秘密鍵を生成する際に(ステップ1)、予め合成数 n 及び前記楕円曲線のパラメータ(a , b)を定め、さらに、合成数 n を法とする剰余演算における楕円曲線 E_n (a , b)上の2点(G_1 , G_2)を定め、 k , n , a , b , G_1 , G_2 を公開鍵とし、合成数 n の素因数を秘密鍵とする。

【0015】また、送信装置において、暗号文を生成する際に(ステップ4)、乱数 γ を生成し、乱数 γ と入力される通信文 m を用いて、楕円曲線 E_n (a , b)上の合成数 n を法とする剰余演算における楕円曲線上の演算を行い、暗号文 c (但し、 $c = mG_1 + \gamma mG_2$)を生成する。

【0016】また、受信装置において、暗号文を復号する際に(ステップ6)、送信装置より受信した暗号文を合成数 n の素因数を法とする剰余演算の要素に分解し、分解された要素に対して、ヴェイユ対演算を行い、ヴェイユ対演算の演算値に対して離散対数問題を解き、離散対数問題の解を中国剰余定理により復号文を生成する。

【0017】図2は、本発明の原理構成図である。

【0018】本発明は、送信装置100と受信装置200間の通信の秘密を保証する公開鍵暗号システムにおいて、楕円曲線上の演算を利用して公開鍵を生成して公開し、秘密鍵を生成し、保持する鍵生成・登録手段250と、送信装置100より受信した暗号文に対して剰余演算及びヴェイユ対演算を行い、ヴェイユ対演算の結果に対して離散対数問題を解くことにより暗号文を平文に復号する復号手段260とを有する受信装置200と、受信装置200から公開鍵を入手し、楕円曲線上の演算を利用して暗号文を生成する暗号文生成手段110を有する送信装置100とを具備する。

【0019】また、上記の鍵生成・登録手段250は、合成数 n 及び楕円曲線のパラメータ(a , b)を定める楕円曲線パラメータ生成手段204と、合成数 n を法と

する剰余演算における楕円曲線 $E_n(a, b)$ 上の2点 (G_1, G_2) を定める楕円曲線上点生成手段203と、楕円曲線パラメータ生成手段204により生成されたパラメータ (a, b) 及び楕円曲線上点生成手段203により生成された2点 (G_1, G_2) を用いて公開鍵 k, n, a, b, G_1, G_2 を生成する公開鍵生成手段205と、合成数 n の素因数を秘密鍵として格納する秘密鍵保持手段230とを含む。

【0020】また、上記の復号手段260は、送信装置100から送信された暗号文 c を合成数 n の素因数を法とする剰余演算の要素に分解する剰余分解手段210と、剰余分解手段210により分解された各要素にヴェイユ対演算を用いて離散対数問題を解き、暗号文を復号する解析手段220とを含む。

【0021】また、上記の解析手段220は、離散対数問題の解を中国人剰余定理により1つの復号文に変換する手段を含む。

【0022】また、上記の暗号文生成手段110は、受信装置200より公開鍵 (k, n, a, b, G_1, G_2) を入力する公開鍵入力手段107と、乱数 γ を生成する乱数生成手段108と、乱数生成手段108により生成された乱数 γ と入力される通信文 m とを用いて楕円曲線 $E_n(a, b)$ 上の演算を合成数 n を法とする剰余演算を行い、通信文 m を暗号文 c （但し、 $c = mG_1 + \gamma G_2$ ）を生成する暗号文演算手段109を含む。

【0023】

【作用】本発明は、楕円曲線の特性である2重周期を利用するものであり、1つの周期を通信文の暗号化に用い、もう一方の周期を確率的に乱数化するために用いる。このように楕円曲線の2重周期を利用することにより、1個の暗号文で暗号化できる通信文のサイズが通信文の暗号化に用いる周期により決定される。

【0024】また、復号処理では、ヴェイユ対（岡本・桜井著「代数幾何学的アルゴリズム」、情報処理、情報処理学会、Vol. 34, No. 2, 2月号(1993)）を利用することにより、乱数成分を除去し、さらに、離散対数問題を求める手法により復号化された通信文を求めることができる。

【0025】

【実施例】図3は、本発明のシステム構成を示す。同図において、送信装置100と受信装置200が通信回線等300を介して接続されている。受信装置200は、鍵生成・登録部250と、復号部260より構成される。鍵生成・登録部250は、素数 p, q の合成数 n 及び楕円曲線のパラメータ (a, b) を設定し、剰余演算における楕円曲線 $E_n(a, b)$ 上の2点 (G_1, G_2) を設定し、合成数 n 、及びパラメータ a, b を公開鍵とし、また、合成数 n の素因数を秘密鍵として保持する。また、復号部260は、入力された暗号文 c を合成数 n の素因数を法とする剰余演算の要素に分解し、分

解された各要素毎に、ヴェイユ演算を用いて離散対数問題の解として通信文 m を計算する。

【0026】最初に受信装置の鍵生成・登録部250について説明する。

【0027】[受信装置：鍵生成・登録部]図4は、本発明の一実施例の受信装置の鍵生成・登録部の構成を示す。受信装置200の鍵生成・登録部250は、素数生成器201、乗算器202、楕円曲線パラメータ生成器203、楕円曲線上点生成器204、剰余定理演算器205、位相計算器206、最小公倍数演算器207より構成される。

【0028】素数生成器201は、素数 p, q を生成し、乗算器202及び楕円曲線パラメータ生成器203及び楕円曲線上点生成器204に出力する。乗算器202は、素数 p, q を乗算し、 $n = pq$ とする。楕円曲線パラメータ生成器203は、入力された素数 p, q を係数 a, b に対し、パラメータ $(a_p, b_p), (a_q, b_q)$ を楕円曲線上点生成器204、剰余定理演算器205及び位相計算機206に出力する。楕円曲線上点生成器204は、楕円曲線パラメータ生成器203より出力されたパラメータ $(a_p, b_p), (a_q, b_q)$ と素数生成器201より出力された素数 p, q により、二重周期 $(G_{1p}, G_{2p}), (G_{1q}, G_{2q})$ を取り出す。

【0029】ここで、楕円曲線とは、素数 p と係数 a, b に対し、
$$y^2 \equiv x^3 + ax + b \pmod{p}$$
を満たす点の集合に無限遠点 O を加えた集合 $E_p(a, b)$ にて定義される曲線をいう。

【0030】次に、剰余定理演算器205は、中国人剰余定理により平文を求めるものであり、楕円曲線パラメータ生成器203より出力されるパラメータ $(a_p, b_p), (a_q, b_q)$ と楕円曲線上点生成器204から出力される二重周期 $(G_{1p}, G_{2p}), (G_{1q}, G_{2q})$ を用いて中国人剰余定理に基づいて a, b, G_1, G_2 を計算する。位相計算器206は、素数生成器201より出力された素数 p, q 、楕円曲線上点生成器204から出力された二重周期 $(G_{1p}, G_{2p}), (G_{1q}, G_{2q})$ と、楕円曲線パラメータ生成器203より出力されたパラメータ $(a_p, b_p), (a_q, b_q)$ を用いて、位数 (N_p, N_q, M_p, M_q) を求める。求められた位数は、最小公倍数演算器207に入力し、位数 N_p, N_q について最小公倍数を計算し、その結果 $LCM(N_p, N_q)$ を合成数 n の素因数とし、秘密鍵として格納する。

【0031】図5は、本発明の一実施例の鍵生成・登録部の動作を説明するためのフローチャートである。

【0032】ステップ101)素数生成器201は、素数 p, q を生成する。

【0033】ステップ102)乗算器202が、素数生

成器201より入力された素数 p 、 q を乗算し、合成数 n を求める。

【0034】ステップ103) 楕円曲線パラメータ生成器203は、素数生成器201より素数 p 、 q が入力されると、楕円曲線のパラメータ (a_p, b_p) 、 (a_q, b_q) を設定する。

【0035】ステップ104) 楕円曲線上点生成器204は、楕円曲線パラメータ生成器203より入力されたパラメータ (a_p, b_p) 、 (a_q, b_q) と素数生成器201より入力された素数 p 、 q により、剰余演算における楕円曲線 $E_n(a, b)$ 上の2点(二重周期 (G_{1p}, G_{2p}) 、 (G_{1q}, G_{2q}))を取り出す。

【0036】ステップ105) 次に、剰余定理演算器205は、楕円曲線パラメータ生成器203より入力されるパラメータ (a_p, b_p) 、 (a_q, b_q) と楕円曲線上点生成器204から入力される二重周期 (G_{1p}, G_{2p}) 、 (G_{1q}, G_{2q}) を用いて中国人剰余定理に基づいて公開鍵 (a, b) 、 (G_1, G_2) を計算する。

【0037】ここで、公開鍵は、

$$a \equiv a_p \pmod{p},$$

$$a \equiv a_q \pmod{q},$$

$$b \equiv b_p \pmod{p},$$

$$b \equiv b_q \pmod{q},$$

$$G_1 \equiv G_{1p} \pmod{p},$$

$$G_1 \equiv G_{1q} \pmod{q},$$

$$G_2 \equiv G_{2p} \pmod{p},$$

$$G_2 \equiv G_{2q} \pmod{q}$$

であるとする。

【0038】ステップ106) 位数計算器206は、素数生成器201より入力された素数 p 、 q 、楕円曲線上点生成器204から入力された二重周期 (G_{1p}, G_{2p}) 、 (G_{1q}, G_{2q}) と、楕円曲線パラメータ生成器203より入力されたパラメータ (a_p, b_p) 、 (a_q, b_q) を用いて、以下の位数を求める。

$$【0039】N_p = \text{ord}_p(G_{1p})$$

$$N_q = \text{ord}_q(G_{1q})$$

$$M_p = \text{ord}_p(G_{2p})$$

$$M_q = \text{ord}_q(G_{2q})$$

上記の位数 N_p は、 M_p の約数であり、 N_q は、 M_q の約数である。

【0040】ステップ107) 最小公倍数演算器207は、ステップ106により求められた位数 N_p 、 N_q により最小公倍数 $\text{LCM}(N_p, N_q)$ を計算する。ここで、 $k+1$ を最小公倍数 $(\text{LCM}(N_p, N_q))$ のビットサイズとする。

【0041】ステップ108) 上記の素数 p 、 q を秘密鍵として保持し、合成数 n 、パラメータ (a, b) 、楕円曲線上の2点 (G_1, G_2) 及び最小公倍数のビットサイズ k を公開鍵とする。即ち、 $\{k, n, a, b, G_1, G_2\}$ を公開鍵として公開する。

【0042】次に、送信装置100について説明する。

【0043】[送信装置]図6は、本発明の一実施例の送信装置の構成を示す。送信装置100は、乱数 γ を生成する乱数発生器108からの乱数 γ と、楕円曲線上の剰余演算を用いて受信装置200に送信したい通信文 m を暗号化し、暗号文 c を出力する楕円曲線演算器109より構成される。

【0044】楕円曲線演算器109は、受信装置200から入力された公開鍵 (n, a, b, G_1, G_2) 、乱数発生器108から入力された乱数 γ 及び通信文 m を用いて、

$$c = mG_1 + \gamma G_2 \text{ over } E_n(a, b)$$

により暗号文 c を求める。ここで、“+”は、合成数 n を法とする剰余演算における楕円曲線上の演算を意味し、 mG_1 は、 $G_1 + G_1 + \dots + G_1$ (m 回)を意味する。楕円曲線上の演算“+”は、 n を法とする剰余四則演算を繰り返し用いることにより実現できる(具体的には、以下の書籍等を参照されたい。N.Koblitz, "A course in number theory and cryptography," GTM-114, Springer-Verlag, New York(1987))。

【0045】図7は、本発明の一実施例の送信装置の動作を示すフローチャートである。

【0046】ステップ201) 送信装置100の乱数発生器108は乱数 γ を発生させる。

【0047】ステップ202) 受信装置200に送信したい平文の通信文 m を入力する。

【0048】ステップ203) 受信装置200で生成された公開鍵 n, a, b, G_1, G_2 を入力する。

【0049】ステップ204) 送信装置100は、乱数 γ 、通信文 m 、公開鍵 n, a, b, G_1, G_2 を用いて、楕円曲線 $E_n(a, b)$ 上の剰余演算を m 回繰り返す。詳しくは、乱数 γ と公開鍵 G_2 を合成して、 γG_2 を生成し、通信文 m と公開鍵 G_1 を合成して mG_1 を生成する。次に、 γG_2 と mG_1 を合成して暗号文 c を生成する。

【0050】ステップ205) 送信装置100は、暗号文 c を出力する。

【0051】次に、受信装置200の復号部260について説明する。

【0052】[受信装置：復号部]図8は、本発明の一実施例の受信装置の復号部の構成を示す。同図に示す受信装置200の復号部260は、剰余演算器210、ヴェイユ対演算器211A、B、離散対数演算器212、及び剰余定理演算器205を有する。このうち、同図においてヴェイユ対演算器211A、211Bの2つが含まれているが、これは、1つの演算器として構成されてもよい。同図では、入出力が2種類あるために区別している。また、剰余定理演算器205は、鍵生成・登録部250の剰余定理演算器205と同様であり、一連の説明のために復号部260内に設けてあるものである。

【0053】剰余演算器210は、送信装置100から送信された暗号文 c が入力されると、合成数 n の素因数を法とする剰余演算の要素 c_p 、 c_q に分解する。この要素 c_p 、 c_q をヴェイユ対演算器211Aに入力する。さらに、楕円曲線上の点 G_{1p} 、 G_{1q} 、 G_{2p} 、 G_{2q} をヴェイユ対演算器211Bに入力する。これによりヴェイユ対演算器211A、211Bはヴェイユ対演算を行い、演算結果を離散対数演算器212に入力する。離散対数演算器212は、鍵生成・登録部250の位数計算器206から位数 N_p 、 N_q が入力され、離散対数の問題の解として復号された通信文 m （平文）が出力される。

【0054】図9は、本発明の一実施例の受信装置の復号部の動作を示すフローチャートである。

【0055】ステップ301）受信装置200の剰余演算器210は、送信装置100から暗号文 c と素数 p 、 q の入力により、以下の剰余演算を行う。

$$【0056】c_p = c \bmod p,$$

$$c_q = c \bmod q$$

を計算する。

【0057】ステップ302）ステップ301で求めた剰余演算結果 c_p 、 c_q と位数計算器206からの出力の楕円曲線上の点の位数 M_p 、 M_q 及び鍵生成・登録部250の楕円曲線上点生成器204により生成された楕円曲線上の点 (G_{2p}, G_{2q}) をヴェイユ対演算器211Aに入力する。また、鍵生成・登録部250の楕円曲線上点生成器204により生成された楕円曲線上の点 (G_{1p}, G_{1q}) 、 (G_{2p}, G_{2q}) 及び楕円曲線上の点の位数 M_p 、 M_q をヴェイユ対演算器211Bに入力する。

【0058】ステップ303）ヴェイユ対演算器221Aは、位数 M_p 、 M_q と剰余演算器210の出力 c_p 、 c_q 及び楕円曲線上の点 (G_{2p}, G_{2q}) を用いて以下のヴェイユ対演算（ヴェイユ対演算の詳細は、岡本・桜井著「代数幾何学的アルゴリズム」情報処理学会誌、2月号（1993）を参照）を行う。

$$【0059】\beta_p = e M_p (c_p, G_{2p})$$

$$\beta_q = e M_q (c_q, G_{2q})$$

これにより、第1のヴェイユ対 β_p 及び β_q を求める。

【0060】さらに、ヴェイユ対演算器221Bは、入力された楕円曲線上の点 (G_{1p}, G_{1q}) 、 (G_{2p}, G_{2q}) 及び楕円曲線上の点の位数 M_p 、 M_q を用いて、以下により第2のヴェイユ対 α_p 、 α_q を求める。

$$【0061】\alpha_p = e M_p (G_{1p}, G_{2p})$$

$$\alpha_q = e M_q (G_{1q}, G_{2q})$$

ステップ304）次に、ヴェイユ対演算器221A、221Bの演算結果 β_p 、 β_q 、 α_p 、 α_q 、最小公倍数 N_p 、 N_q 、素数 p 、 q を離散対数演算器212に入力する。

【0062】ステップ305）離散対数演算器212は、入力された β_p 、 β_q 、 α_p 、 α_q 、最小公倍数 N

p 、 N_q 、素数 p 、 q を用いて、以下の式を満足する離散対数の解 m_p 、 m_q を求める。

$$【0063】\beta_p = \alpha_p^{m_p} \bmod p$$

$$\beta_q = \alpha_q^{m_q} \bmod q$$

なお、上記の最小公倍数 N_p 、 N_q は上記の式から消えているが、 α_p 、 α_q の位数が N_p 、 N_q という事実を用いて m_p 、 m_q を求めるための入力として必要である（詳細は、池野・小山著「離散対数問題のポーリック・ヘルマン・アルゴリズム」参照）。

【0064】ステップ306）離散対数演算の解 m_p 、 m_q 及び素数 p 、 q を中国人剰余定理演算器205に入力する。

【0065】ステップ307）中国人剰余定理演算器205は、素数を用いて中国人剰余定理により平文 m を求める。

$$【0066】$$

$$m \equiv m_p \pmod{N_p}, \quad \dots \quad ①$$

$$m \equiv m_q \pmod{N_q} \quad \dots \quad ②$$

上記の①及び②を合成することにより、平文 m を導出する。

【0067】上記の実施例のように、従来とは全く異なる数学的手段である楕円曲線を用いて暗号化及び復号化を行うものである。例えば、合成数 n を500ビット程度であるとする、暗号文 c は1000ビット程度となる。

【0068】また、ビットサイズ k を例えば、100ビット程度にすることが可能であるため、100ビットの平文を1000ビットの暗号文に変換することが可能である。従来は、1ビットの平文に対して500ビットの暗号文となっていたため、通信効率 $1/500$ であったが、本発明によれば、 $100/1000 = 1/10$ に向上させることができる。

$$【0069】$$

【発明の効果】上述のように、本発明によれば、パラメータを適当に選ぶことにより、適当な大きさのビットサイズ k に対して k ビットの通信文を1つの暗号文 c に暗号化できる。

【0070】また、復号化処理は、ヴェイユ対演算と離散対数演算が大部分を占めるが、ヴェイユ対演算は、文献（岡本・桜井著「代数幾何学的アルゴリズム」情報処理、情報処理学会、Vol.34, No.2, 2月号（1993））で述べられているように、効率的に（ k の多項式のオーダー）で計算できる。また、 N_p 及び N_q が小さな素因数のみを含むようにすれば、離散対数演算も効率的に（ k の多項式のオーダー）で計算できる。

【0071】これにより、従来の方式に比べて、本発明は、通信効率と復号処理効率が共に向上する。

$$【図面の簡単な説明】$$

【図1】本発明の原理を説明するためのシーケンスチャートである。

10

20

30

40

50

【図 2】本発明の原理構成図である。

【図 3】本発明のシステム構成図である。

【図 4】本発明の一実施例の公開暗号システムの受信装置の構成図である。

【図 5】本発明の一実施例の鍵生成・登録部の動作を説明するためのフローチャートである。

【図 6】本発明の一実施例の送信装置の構成図である。

【図 7】本発明の一実施例の送信装置の動作を示すフローチャートである。

【図 8】本発明の一実施例の受信装置の復号部の構成図 10 である。

【図 9】本発明の一実施例の受信装置の復号部の動作を示すフローチャートである。

【符号の説明】

100 送信装置

107 公開鍵入力手段

108 乱数生成手段

109 暗号文演算手段

110 暗号文生成手段

200 受信装置

201 素数生成器

202 乗算器

203 楕円曲線上点生成手段、楕円曲線パラメータ生成器

204 楕円曲線パラメータ生成手段、楕円曲線上点生成器

205 公開鍵生成手段、剰余定理演算器

206 位数計算器

207 最小公倍数演算器

210 剰余分解手段、剰余演算器

211 ユークリッド演算器

212 離散対数演算器

220 解析手段

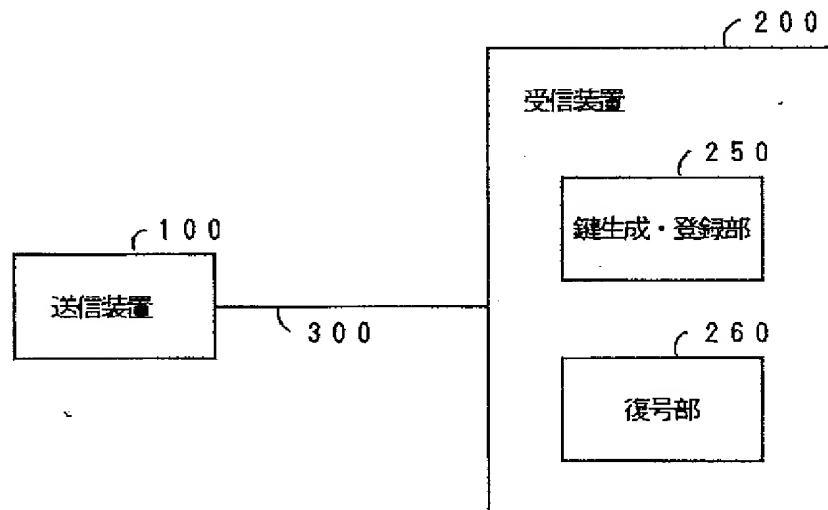
230 秘密鍵保持手段

250 鍵生成・登録手段、鍵生成・登録部

260 復号手段・復号部

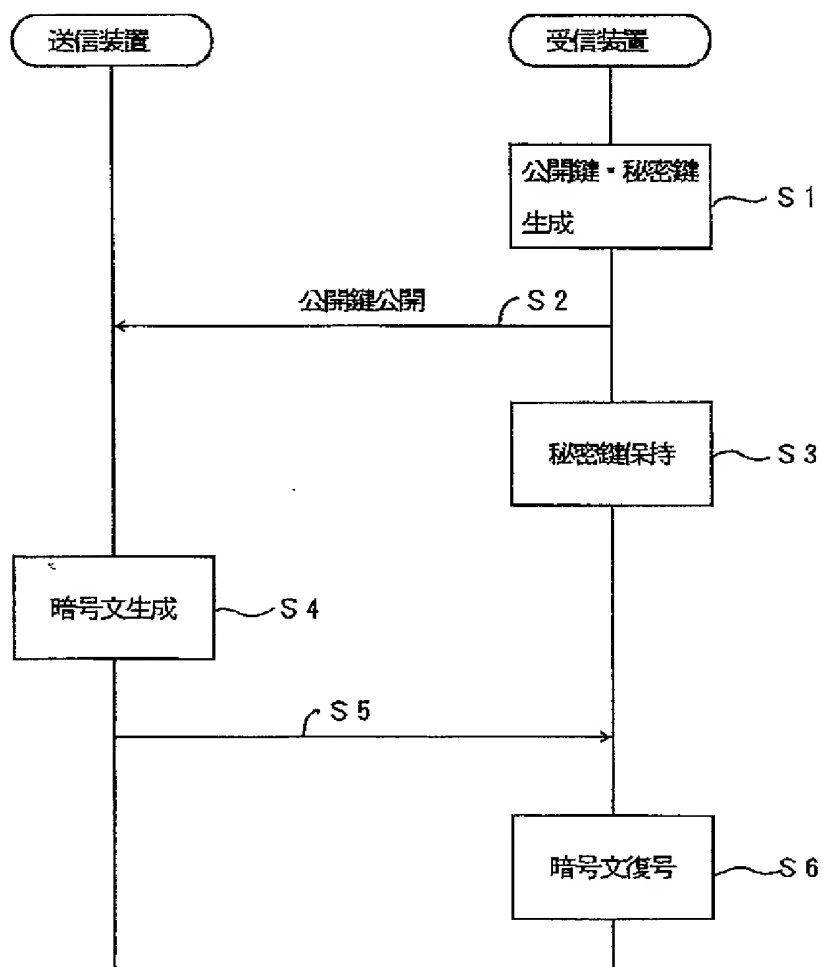
【図 3】

本発明のシステム構成図



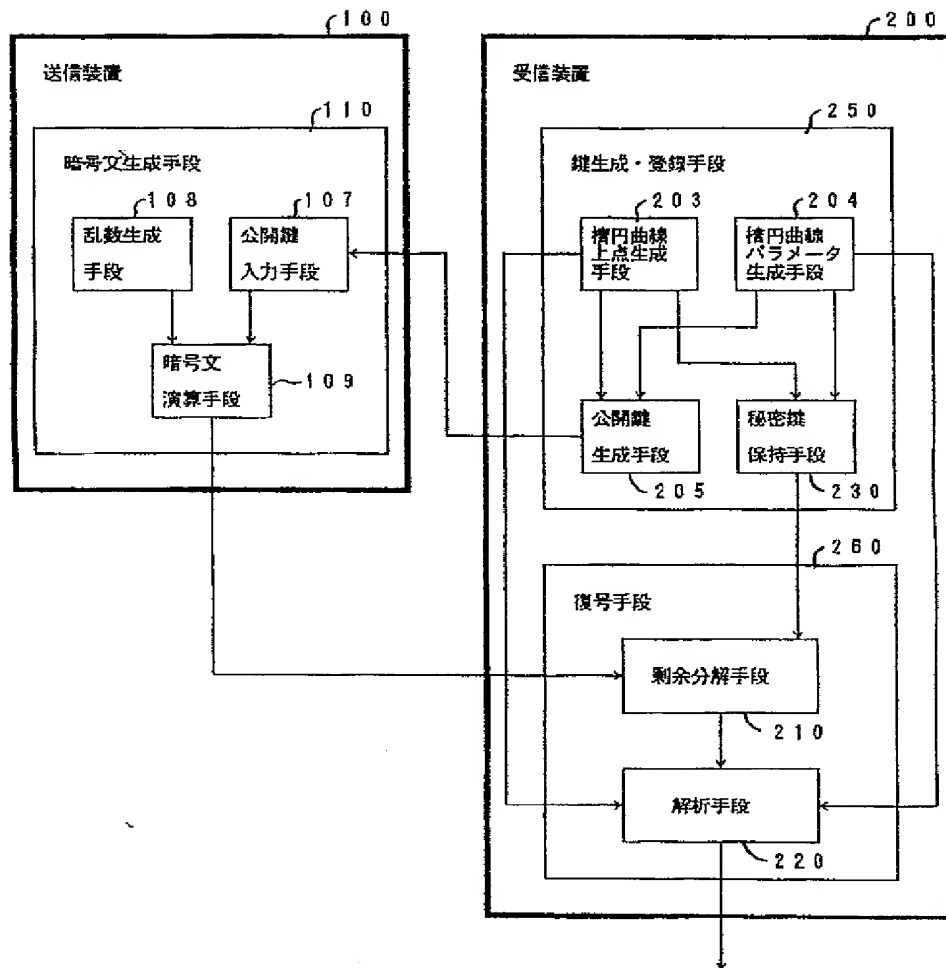
【図 1】

本発明の原理を説明するためのフローチャート



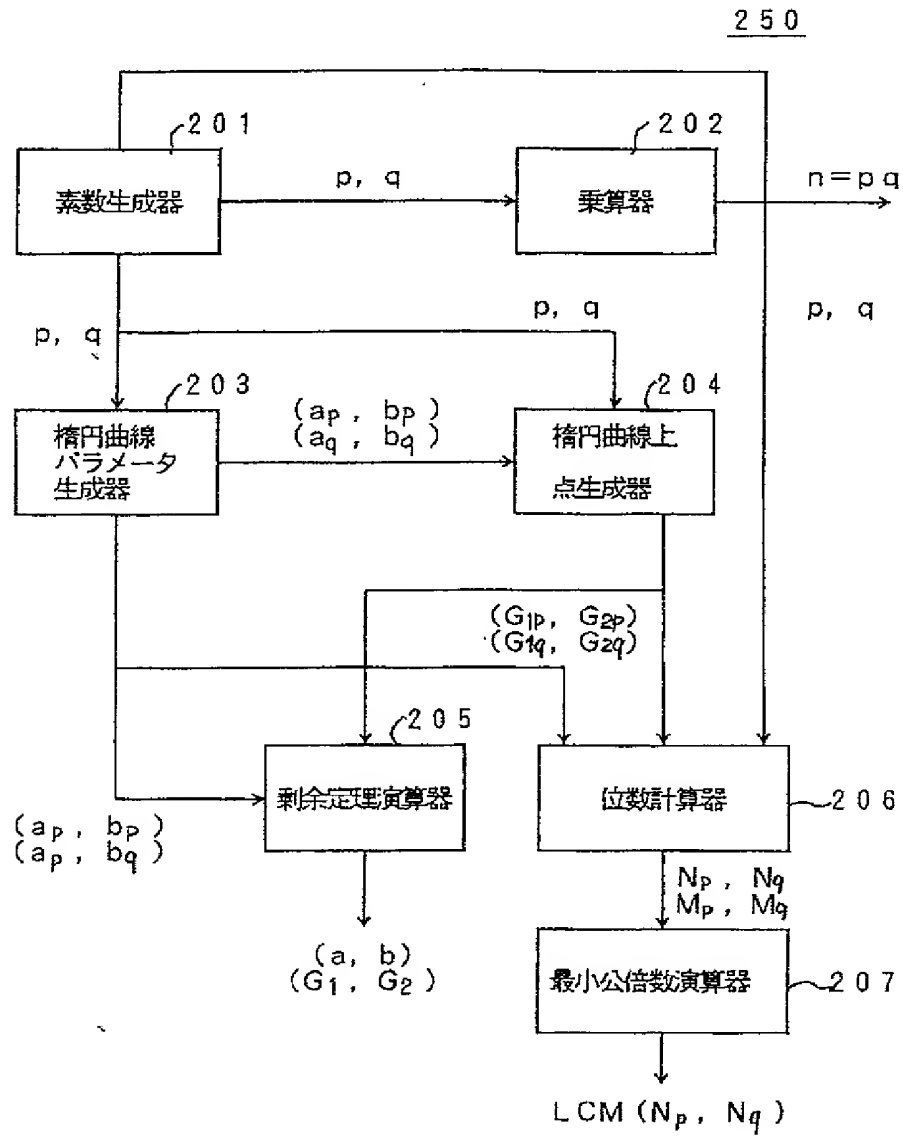
【図2】

本発明の原理構成図



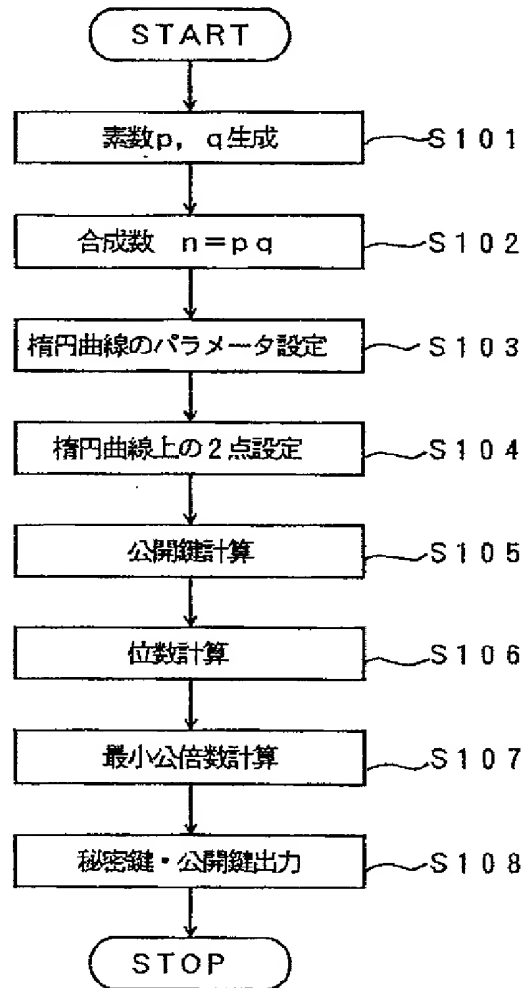
【図4】

本発明の一実施例の公開鍵暗号システムの受信装置の構成図



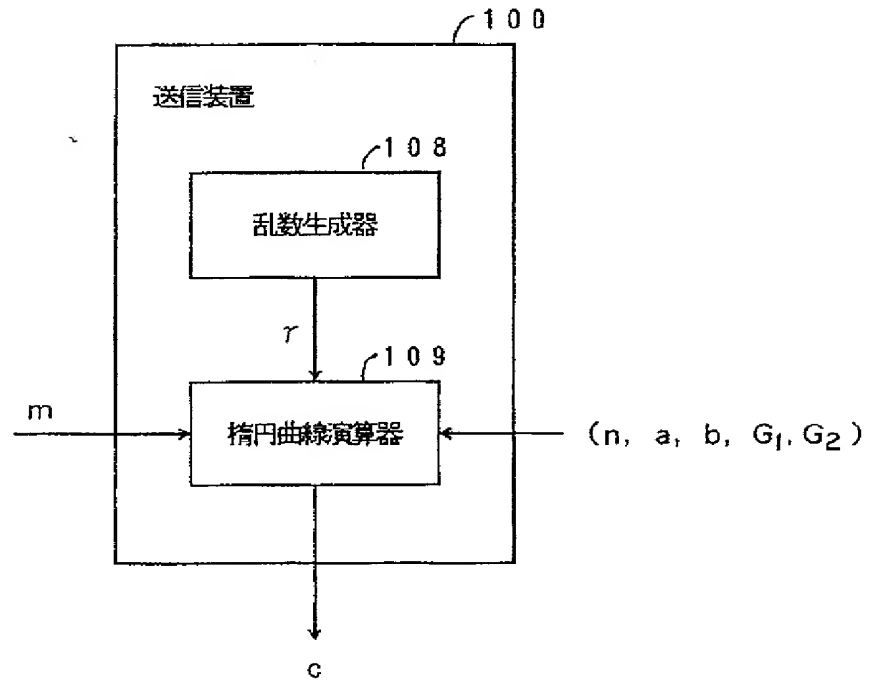
【図 5】

本発明の一実施例の鍵生成・登録部の動作を説明するためのフローチャート



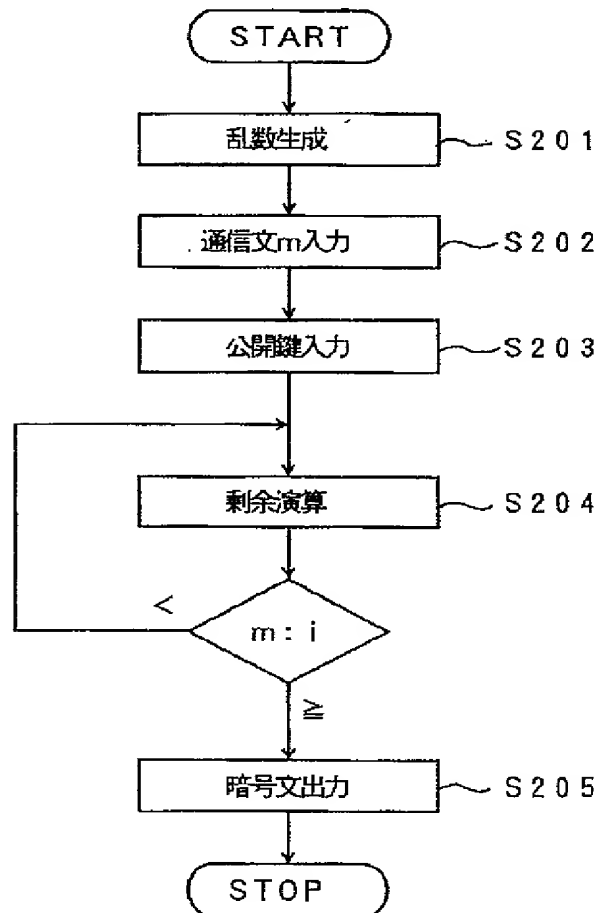
【図 6】

本発明の一実施例の送信装置の構成図



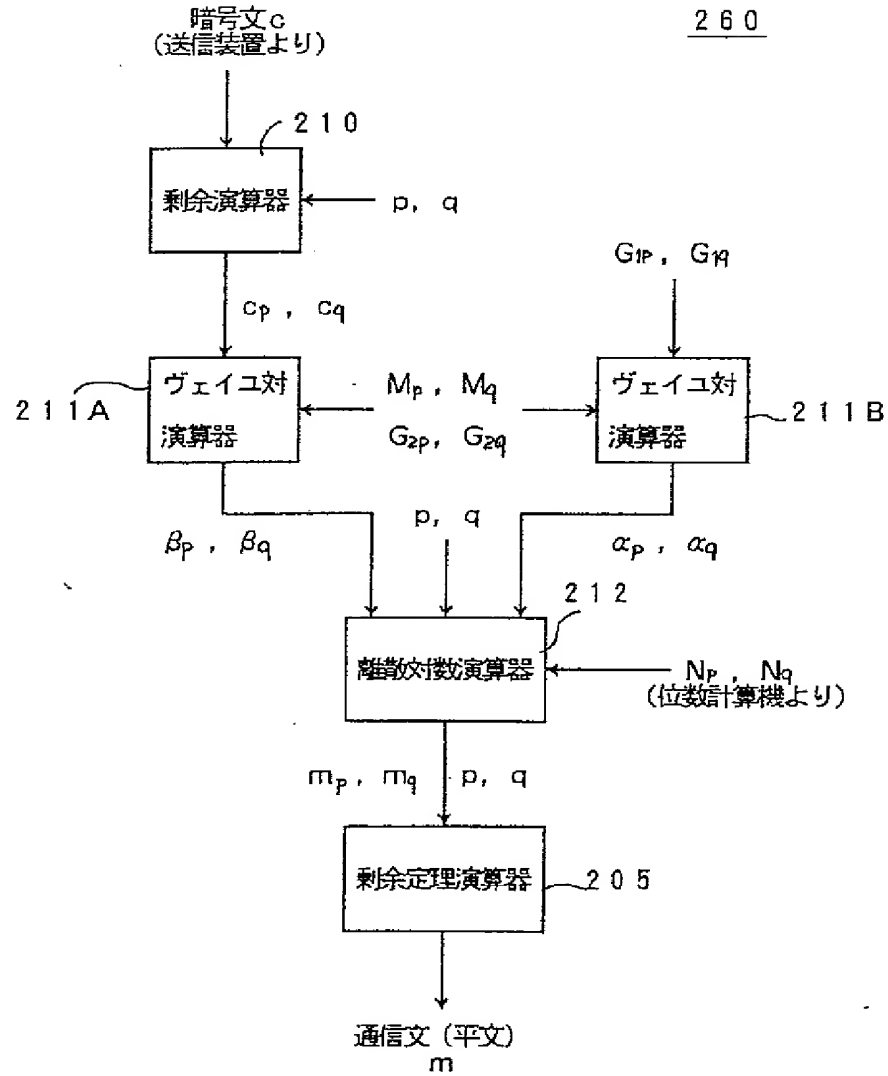
【図 7】

本発明の一実施例の送信装置の動作を示すフローチャート



【図 8】

本発明の一実施例の受信装置の復号部の構成図



【図 9】

本発明の一実施例の受信装置の復号部の動作を示すフローチャート

